UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of

Information associated with Kik username "hughmungiss" stored at the premises owned, maintained, controlled, and operated by MediaLab, Inc., 1237 7th Street, Santa Monica, California 90401

Case No. 1:21-mj-00027

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A to the accompanying Affidavit.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B to the accompanying Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A(a)(5)(B) and (a)(2)(A)	Possession and Distribution of Child Pornography

The application is based on these facts:

See accompanying Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Alicia Boppe
Applicant's signature

Alicia Boppe, Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P 4.1 by (telephone)

Signed: April 23, 2021

W. Carleton Metcalf
United States Magistrate Judge

Date: 4/23/2021

City and state: Asheville, North Carolina — The Hon. W. Carleton Metcalf, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISON

IN RE SEARCH OF:	)	
	)	
INFORMATION ASSOCIATED WITH	)	
THE KIK USERNAME,	)	
"HUGHMUNGISS"	)	Case No. **1:21-mj-00027**
THAT IS STORED AT PREMISES	)	
CONTROLLED BY	)	
MEDIALAB INC. 1237 7th ST., SANTA MONICA	)	
CALIFORNIA 90401	)	

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Alicia Boppe, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2018. As a Special Agent with the FBI, I have managed investigations into criminal and counter-intelligence matters, conducted interviews, evidence searches, surveillances, arrest operations, electronic monitoring, and general investigative research. I have continued my professional education through in-service and online courses, to include counter-intelligence, case management, operation of confidential sources, and investigative research methods. Prior to joining the FBI, I worked as the Director of Environmental Health Safety and Regulatory Affairs for a chemical manufacturing company for two years. I have also worked as an environmental scientist in both the research and consulting industries, involving permitting, regulatory practice, and business management. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws and I am authorized by the Attorney General to request a criminal complaint and arrest warrant.

2. This affidavit is submitted in support of an application for a search warrant for information associated with the Kik Username "hughmungiss" (the "SUBJECT KIK ACCOUNT"), that is stored at the premises owned, maintained and operated by MediaLab, Inc., a company headquartered at 1237 7th Street, Santa Monica, California 90401, which functions as an electronic communications service and remote computing service, and is a provider of electronic and remote computing services. This affidavit is submitted under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), and Rule 41, Federal Rules of Criminal Procedure, requiring MediaLab, Inc., to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the SUBJECT KIK ACCOUNT, referenced in this affidavit and further described in Attachment A, including the contents of communications, which represent evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2251(d)(1)(A)(advertisement of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography). The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of the facts known by me about this investigation.

3. I have probable cause to believe that evidence of violations of 18 U.S.C. §2251(d)(1)(A)(advertisement of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and

distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography) involving the use of a computer and the Internet, is located in and within the aforementioned account. I have probable cause to believe that the member account that is the subject of this application will have stored information and communications that are relevant to this investigation, including evidence of the identity of the person maintaining the account associated with the SUBJECT KIK ACCOUNT. Based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the account.

STATUTORY AUTHORITY

4. The legal authority for this search warrant application is derived from Rule 41, Federal Rules of Criminal Procedure and Title 18, United States Code, Sections 2701 et seq., titled "Stored Wire and Electronic Communications and Transactional Records Access."

5. Title 18, United States Code, Section 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703(a) & (b), as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

DEFINITIONS

6. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators,

electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" may refer to an IP address of "149.101.1.32." Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

l. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup

Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. A "Preservation Letter" is a letter that a government entity may issue to internet service providers pursuant to Title 18, United States Code, Section 2703(f), to ensure that the internet service providers preserve records in their possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

n. "Cloud storage" is an online central storage location, which allows users to access their files from anywhere using a device connected to the Internet.

o. “iCloud” is a cloud storage and cloud computing service from Apple Inc. The service allows users to store data on remote computer servers for download to multiple devices, to include smart phones and computers.

p. “Instant messaging” is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating and gaming websites and mobile applications offer instant messaging for users to communicate amongst themselves. More advanced features of instant messaging include push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

q. A “hash value” is value given to a file or data after a mathematical function converts the data into an alpha-numeric value. A hash value is akin to a digital fingerprint, in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. A hash value is unique to the specific data from which the hash value was generated. Hash values can be used to search for identical data stored on various digital devices, as identical data will have the same hash value.

r. A "URL" defined as a Uniform Resource Locator is a protocol for specifying addresses on the internet.

COMPUTERS AND CHILD PORNOGRAPHY

7. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has radically changed the way that child pornographers obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

9. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos

indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

11. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, Apple Inc., and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also

be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging."

14. Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communication, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

15. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving

individuals, who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents in the area of investigating cases involving sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

16. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

17. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

INFORMATION REGARDING KIK MESSENGER

18. Kik Messenger (hereinafter, "Kik") is a free instant messaging mobile application designed and previously owned by Kik Interactive Incorporated, a company based in Waterloo, Canada[1]. Kik uses the Internet to allow users to send and receive instant messages, photos and videos. During the account registration process, users are prompted to create a username, which cannot later be changed, and a display or vanity name, which other users initially see when communicating. During the registration process, users are also asked to provide an email address, date of birth, user location and a profile picture. Email addresses can be "confirmed,"

[1] Kik was purchased in or about October 2019 by MediaLab, Inc., a U.S.-based technology company headquartered in California.

which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or "unconfirmed," which means the email address is invalid, or the user did not click on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process.

19. Once an account is created, a user is able to locate other users through a search feature. The search feature generally requires a user to know an intended recipient's username to locate them. Once connected, Kik users can share messages, images, and videos. Kik also allows users to create chatrooms, through which groups of up to 50 users can exchange messages and digital files. These chatrooms, commonly referred to as "Kik Groups," are administered by the user who created the chatroom, and this user has the authority to add, remove, and ban other users from the group, as well as to promote other users to "administrator." This is true for both private and public chatrooms. Many public groups are created with a group code that contains a "hashtag" (e.g., "#KikTeens"), allowing the group or chatroom to be located more easily.[2] Specifically, a user will search for a public group using a term or word associated with the group name, which is often contained in the hashtag. Once a group is created, Kik users can engage in a "group chat" and exchange messages and content.

20. According to Kik's Terms of Service, which each user must acknowledge when creating an account, it is a violation of the agreement to use Kik to upload, post, comment on, or store content that is obscene, offensive, contains pornography, or is harmful to minors in any way. These Terms of Service specifically state that "…[Kik] may review, screen and delete your User Content at any time if we think it may violate these Terms. You are responsible for the User Content that you send through the Services, including for back up of such content."

[2] The hashtag locating feature is not typically available for private groups.

21. To combat the proliferation of child pornography on its platform, the Kik Trust and Safety Team uses a third-party company to review profile pictures that are uploaded by users and groups. Kik also uses PhotoDNA to compare user-uploaded images against a database of known child pornography images that are in circulation. Any images that are flagged and reported by the third-party company or the PhotoDNA software are subsequently viewed by a member of the Kik Trust and Safety Team.

22. Kik also allows users to report other users who have abused or harassed them within the app. These are referred to as "Abuse Reports." When a Kik user submits an Abuse Report, they can include their full conversation history, including text and any images or videos transmitted in the conversation. When Kik receives an Abuse Report, an employee reviews the reported material to verify that it contains child pornography or is otherwise considered child exploitative material.

23. Any material determined by Kik to be exploitative through PhotoDNA hash match, third-party monitoring, or Abuse Reports is subsequently reported to the National Center for Missing and Exploited Children ("NCMEC") via a CyberTipline referral. Kik provides NCMEC with the reported material, as well as basic subscriber information for the suspect account. This subscriber data includes, but is not limited to, the information entered by the user during the account registration process, any updates to this information after the registration process, device type (e.g., iPhone, Samsung Galaxy S5, etc.,), the Kik application version used, and log-in data associated with the last thirty days of account activity. Upon reporting this information to NCMEC, Kik deletes or disables the suspect account for violating its Terms of Service.

24. Based on my training and experience in child exploitation investigations, I am aware that Kik is a prominent meeting place for individuals seeking to share child pornography and engage in child exploitative dialogue. I have investigated several offenders who used Kik to transport, distribute, and receive child pornography. Based on information obtained from interviews with some of these offenders, I am aware that Kik is a preferred platform for child exploitation offenders because the application facilitates anonymous communication, which assists offenders in avoiding detection by law enforcement.

FACTS IN SUPPORT OF PROBABLE CAUSE

25. In December 2020, an undercover FBI agent with the Miami FBI Field Office was conducting surveillance on the messaging application Kik and identified user "hughmungiss" as being a member of "Group 1."[3] Additionally, the agent observed "hughmungiss" share child pornography within the group. In reviewing the materials provided by the undercover agent, your affiant observed at least four (4) instances in which "hughmungiss" distributed child pornography to the group:

a. On December 10, 2020, "hughmungiss" sent an image to the group of an adult male using his erect penis to penetrate the anus of a naked pubescent male.

b. On December 12, 2020, "hughmungiss" sent an image to the group of a prepubescent female in red stockings with her legs spread apart in the air and being penetrated by an adult male.

[3] The true name of "Group 1" is known by your affiant. Additionally, "Group 1" was observed by your affiant as being a Kik chat group that involves the sharing of child pornography. The group name is not being revealed due to it being involved in an ongoing investigation.

c. On January 14, 2021, “hughmungiss” sent an image to the group of a prepubescent female laying between an adult male’s legs, performing oral sex on the adult male while he holds her head with his hand.

d. On January 20, 2021, “hughmungiss” sent a video to the group of a female infant with her legs up and an adult male penetrating her anus with his erect penis multiple times. The infant can be heard crying.

26. On December 11, 2020, Kik user “hughmungiss” made a post to the “Group 1” chat group stating that he had lost all his videos when he deleted the Kik application and then later reinstalled it.

27. On January 7, 2021, the FBI Miami Field Office submitted an administrative subpoena to Kik via MediaLab, Inc. requesting subscriber information associated with user “hughmungiss.”

28. On or about January 15, 2021, Kik responded to the administrative subpoena request and provided the following subscriber information connected to the “hughmungiss” user account:

January 10, 2021 First Name: Ben
January 10, 2021 Last Name: Dover
December 17, 2020 First Name: .
December 17, 2020 Last Name: .
February 22, 2020 First Name: Rod
February 22, 2020: Hander
Email: jeffdurst945@gmail.com
Username: hughmungiss
Device Type: Android
Birthday: March 31, 1970
User Location on January 14, 2021 at 22:30:14 UTC: IP: 174.80.215.196

29. On January 19, 2021, the FBI Miami Field Office sent an administrative subpoena to Spectrum/Charter Communications requesting information associated with IP address 174.80.215.196 from January 14, 2021 at 22:27:13 UTC.

30. On January 22, 2021, Spectrum/Charter Communications responded to the administrative subpoena request with the following information associated with IP address 174.80.215.196:

> Subscriber Name: Jeffrey Culp
> Service Address: 24 Willow Ct., Asheville, NC 28805
> Email: jeffdurst945@gmail.com
> Telephone Numbers: 828-200-2606

31. On or about January 25, 2021, the FBI Miami Field Office received results from a Department of Motor Vehicles (DMV) database check for Jeffrey CULP. The results showed a suspended Ohio driver's license along with an image of CULP that appeared to be the same individual in the profile picture for the Kik user "hughmungiss." The return also noted CULP had an active arrest warrant out of Ohio for a traffic related offense.

32. On or about February 1, 2021, the Miami FBI Division notified the Asheville, North Carolina FBI Resident Agency regarding the distribution of child pornography by CULP utilizing the Kik username "hughmungiss."

33. On March 5, 2021, an employment check was completed for CULP. Results indicated a home address of 24 Willow Ct., Asheville, North Carolina 28805, and a listed email address of jeffdurst945@gmail.com.

34. Also, on March 5, 2021, a law enforcement database was reviewed by your affiant for CULP. Results showed a date of birth of March 30, 1970, and multiple addresses including, 9723 E Center St. Apartment A, Windam, Ohio 44288, and 24 Willow Ct., Asheville, North Carolina 28805.

35. That same day, your affiant received North Carolina DMV database results for CULP and found expired driver's license information including a photograph. In comparing the photograph on the driver's license with the Kik profile image for "hughmungiss" the images appeared to be of the same individual.

36. On March 18, 2021, your affiant served MediaLab, Inc., with a preservation letter for the records related to "hughmungiss" and the SUBJECT KIK ACCOUNT.

37. On March 18, 2021, your affiant received a response from MediaLab, Inc., acknowledging the receipt and preservation of the SUBJECT KIK ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab, Inc. to disclose to the government copies of the records and other information (including the content of the communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

39. Based on my training and experience, and the facts as set forth above, I submit I have probable cause to believe that on the computer systems in control of MediaLab, Inc., there exists evidence of a crime(s), contraband and/or fruits of a crime(s). Specifically, I have probable cause to believe that Kik user account "hughmungiss" (the SUBJECT KIK ACCOUNT), described in Attachment A, will contain evidence, fruits, and instrumentalities of a crime(s), that is violations of 18 U.S.C. §2251(d)(1)(A)(advertisement of child pornography); 18

U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography). Accordingly, a search warrant is requested.

40. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711(3), and Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." Title 18, United States Code, Section 2711(3)(A)(i).

41. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

/S/ Alicia Boppe
Date: April 22, 2021
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 23rd day of April, 2021, at 4:10 P.M.

Signed: April 23, 2021

W. Carleton Metcalf
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to information associated with the SUBJECT KIK ACCOUNT, Kik username hughmungiss, which is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company headquartered at 1237 7th Street, Santa Monica, California 90401.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of MediaLab, Inc. (hereafter, "MediaLab") to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to MediaLab personnel by law enforcement agents. MediaLab personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files associated with username hughmungiss, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. MediaLab system administrators will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. MediaLab will disclose responsive data by sending to the following recipient using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. §2252, 2252A or similar statute or code: Special Agent Alicia Boppe, FBI –151 Patton Ave, Suite 211 Asheville, NC 28801.

I: Information to be disclosed by MediaLab

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any content, messages, records, files, logs or information that has been deleted but is still available to MediaLab, or has been preserved, MediaLab is required to disclose the following information to the government for the account listed in Attachment A, for the period of **February 22, 2020, to the present**. Such information should include the following:

1. Any and all subscriber data for user hughmungiss including usernames, first and last name, contact information and email address, profile or background photo, device information, account creation information, IP address logs, and registration information (birth date, email address, and IP address);

2. Any and all content from the transactional chat log, chat platform log, roster log, abuse reports, content ID data, and email events sent or received by this user, which have not been deleted from MediaLab servers;

3. Any and all photographs or videos sent or received by this user, including from both individual and group chats, which have not been deleted from MediaLab servers;

4. Any and all location data relating to this user available on MediaLab servers;

5. All records or other subscriber information related to this user stored on MediaLab servers, including, but not limited to, account creation date, account access information with IP logs and timestamps, email address(es), date of birth, associated mobile number, and mobile device information;

6. All content and records currently being preserved by MediaLab pursuant to a Preservation Request submitted on March 18, 2021.

II: Information to be seized by the Government

All information described above in Section I, including correspondence, records, documents, photographs, videos, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §2251(d)(1)(A)(advertisement of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

1. Any person knowingly transporting, receiving, distributing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);

2. Any person discussing the distribution or receipt of child pornography, or the sexual abuse of children.

3. Credit card and other financial information including but not limited to bills and payment records;

4. Evidence of the identity of the individual(s) who used, owned, or controlled the account or identifier listed on Attachment A;

5. Evidence of the times the account or identifier listed on Attachment A was used;

6. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.